**УДК 342.924:004.056**

**Организационно-правовой механизм обеспечения информационной безопасности**

**Organizational and legal mechanism for ensuring information security**

Степенко В.Е. - д.ю.н., доцент,

директор юридического института ТОГУ

Карабанов Д. Е. - студент 4 курса ЮИ Тихоокеанского Государственного Университета – по специальности ПОНБ (с)-51 г. Хабаровск.

Stepenko V.E. – Doctor of Law, Associate Professor,

Director of the Law Institute of PNU

Karabanov D. E. - 4th year student of the South Pacific Institute of the Pacific State University, majoring in PHC (s) -51, Khabarovsk

В научной работе проанализированы общие теоретические аспекты обеспечения информационной безопасности, рассмотрены существующие угрозы в указанной сфере, научные подходы к их определению и классификации. На основании проведенного исследования определены основные компоненты организационно-правового механизма обеспечения информационной безопасности с учетом особенностей свойств информации, циркулирующей в информационной среде.

The scientific work analyzes the general theoretical aspects of information security, examines the existing threats in this area, scientific approaches to their definition and classification. On the basis of the conducted research, the main components of the organizational and legal mechanism for ensuring information security have been determined, taking into account the characteristics of the properties of information circulating in the information environment.

**Ключевые слова:** Информация, механизм, организационные меры, информационная безопасность, угрозы, ущерб, свойства информации.

**Keywords**: Information, mechanism, organizational measures, information security, threats, damage, properties of information.

В настоящее время не существует единого определения информации как научного термина. С точки зрения юриспруденции информация это сведения (сообщения, данные) независимо от формы их представления. Что касается термина информационная безопасность, то это практика или своего рода процесс предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Данная практика обеспечивает конфиденциальности, целостности и доступности информации разного рода.

Обеспечение безопасности, в частности информационной сводится к потребности в создании организационных, материальных, правовых и иных условий, позволяющих достичь поставленные цели и задачи.

Так как информационная сфера - это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, то она нуждается в адекватном и современном правовом регулировании. В настоящий момент данная сфера регулируется Федеральным законом от 27.07.2006 N 149 “Об информации, информационных технологиях и о защите информации’’. [/4/](#тема_2) Данный закон говорит о создание необходимой правовой основы для реализации конституционных прав граждан, защиты общественных и государственных интересов в сфере использования современных информационных технологий. Главной целью он ставит перед собой установить основные правила и перечень способов защиты публичных и гражданских прав на информацию, защиты самой информации путем принятия основных правовых, организационных и технических (программно-технических) мер по ее защите, также законодательно закрепить принципы использования информационно-телекоммуникационных сетей, в том числе при международном информационном обмене.

Если затрагивать вопросы административно-правового регулирования указанных отношений, то они достаточно обширны. Чтобы раскрыть административно-правовые аспекты обеспечения информационной безопасности, необходимо отношения по обеспечению информационной безопасности рассматривать как предмет правового регулирования административного права. В комплексе правовых мер обеспечения информационной безопасности особое место занимает административно-правовое регулирование информационной безопасности, которое может быть направлено на определение структуры данных отношений, процесса управления ими, разработки принципов, средств, мер и методов осуществления данной деятельности, т.е. вообще установления информационного режима. Также еще один вектор административно-правового регулирования данных отношений направлен на предупреждение и пресечение противоправных посягательств на охраняемые законом информационные источники.

Помимо этого, в большинстве работ, где исследуется обеспечение безопасности, и в частности информационной, с юридической точки зрения речь идет о национальной безопасности и о национальных интересах в информационной сфере как основном объекте информационной безопасности [/16/](#тема_12). Нормативные правовые акты регламентируют совокупность сбалансированных интересов личности, общества и государства и обеспечение их безопасности, в том числе в информационной сфере. И лишь немногочисленные работы и ведомственные акты освещают вопросы обеспечения безопасности, в том числе информационной и других объектов.

Следует заметить, что в процессе обеспечения безопасности осуществляется охрана именно законных интересов. Соответственно основным объектом в частности информационной безопасности также являются законные интересы. Законный интерес – потребность субъекта в осуществлении его прав и свобод.

Гольтяпина И.Ю. отмечает, что категория «законного интереса» выполняет функцию обобщения. Использование термина «законный интерес» указывает на то, что безопасность должна быть обеспечена не в тот момент, когда происходит опосредование прав и свобод в конкретном правоотношении, а по факту возможности такого опосредования, поскольку законный интерес – это потребность, которая может возникнуть. Законный интерес должен кем-то реализовываться и кто-то должен быть его носителем, обладателем. Выявив «носителя» мы сможем определить, кого надо защищать, чтобы не был нарушен его законный интерес. При определении их административно-правового статуса становится возможным не только организовать четкую внутриорганизационную их деятельность, но главное – создать некую иерархическую структуру обеспечения информационной безопасности на любом управленческом уровне: в общегосударственном масштабе, в рамках субъекта Российской Федерации, в конкретном учреждении, предприятии или организации.

В информационной сфере можно выделять законные интересы:

– физических лиц (граждане РФ, иностранные граждане, лица без гражданства, должностные лица и т.д.);

– организаций (коммерческие и некоммерческие юридические лица всех организационно-правовых форм, организации без образования юридического лица, в том числе иностранные, государственные органы и т.д.);

– Российской Федерации, субъектов РФ и муниципальных образований.

Практически такой же состав носителей законных интересов – объектов обеспечения информационной безопасности отмечает А.С. Саввин, конкретизируя, что информационная безопасность должна обеспечиваться для всех экономических агентов и хозяйствующих субъектов, т.е. населения – основного носителя информации, предприятий и организаций, а также для государства в целом.

Однако чтобы обеспечить информационную безопасность носителей законных интересов необходимо обеспечить защиту каких-то конкретных предметов, повреждение или доступ к которым могут повлечь неблагоприятные последствия для носителя и нарушение охраняемых законных интересов. Следовательно, непосредственными объектами обеспечения информационной безопасности выступают правоотношения, имеющие как материальное, так и нематериальное предметное воплощение. Они возникают по отношению как к предметам, имеющим материальное выражение – компьютер, помещение и т.п., так и к предметам нематериального характера – достоинство, честь и т.п. Выделим наиболее общие непосредственные объекты информационной безопасности:

а) зависящие от информационных отношений права, свободы и законные интересы физических лиц, организаций, Российской Федерации, субъектов Российской Федерации и муниципальных образований;

б) помещения, где распространяется информация, материальные ценности и финансовые средства, которые находятся в ведении физических лиц, организаций, Российской Федерации, субъектов Российской Федерации и муниципальных образований и информация о них;

в) информационно-вычислительные центры, научно-исследовательские учреждения и учебные заведения, где содержатся специальные сведения, их информационное, техническое, программное и нормативное обеспечение;

г) информационные технологии, информационные системы, информационно-телекоммуникационные сети;

д) система обеспечения информационной безопасности;

е) информация;

ж) репутация и другие.

Стоит отметить, что основным нормативным правовым актом, регулирующим отношения по обеспечению информационной безопасности, к примеру, таможенных органов, является Распоряжение Правительства РФ от 28.12.2012 N 2575-р “О Стратегии развития таможенной службы Российской Федерации до 2020 года” (ред. от 10.02.2018) [/8/](#о_стратегии)

В действующей на настоящее время Стратегии развития таможенной службы Российской Федерации дается определение информационной безопасности таможенных органов, отражающее государственную направленность защищаемых интересов. Под информационной безопасностью таможенных органов РФ понимается состояние защищенности национальных интересов государства в информационной сфере деятельности таможенных органов РФ. Также указывается, что целью обеспечения информационной безопасности таможенных органов РФ является защита этих интересов при осуществлении ФТС России функций по выработке государственной политики и нормативному правовому регулированию, контролю и надзору в области таможенного дела, а также функции агента валютного контроля и специальных функций по борьбе с контрабандой, иными преступлениями и административными правонарушениями.

Обеспечение информационной безопасности является сложным комплексным понятием, охватывающим большой круг процессов и явлений, связанных с противодействием угрозам безопасности в информационной сфере.

Организация межведомственного взаимодействия органов таможни с федеральными органами исполнительной власти осуществляется по нескольким ключевым направлениям. Для целей обеспечения деятельности ФТС России организовано межведомственное информационное взаимодействие с заинтересованными федеральными органами исполнительной власти по следующим основным направлениям: информационный обмен, осуществляемый в рамках соглашений об информационном взаимодействии; информационный обмен в целях реализации федерального закона от 27.07.2010 № 210-ФЗ “Об организации предоставления государственных и муниципальных услуг” [/5/](#об_организации) информационный обмен в целях реализации контрольных функций, осуществляемых таможенными органами. В настоящее время ФТС России подписано 32 соглашения с федеральными органами исполнительной власти и другими ведомствами (Банк России, Федеральное Казначейство и др.) Из них только с 18 министерствами и ведомствами организован непосредственный обмен информацией. С некоторыми ведомствами ведутся работы по согласованию технических условий информационного взаимодействия для дальнейшей практической реализации обмена в соответствии с заключенными соглашениями. Наиболее активный информационный обмен ФТС России осуществляет с ФНС России, Минпромторгом России, Роспотребнадзором, Росздравнадзором, Ростехрегулирование, а также с Банком России и Федеральным Казначейством. Межведомственный информационный обмен осуществляется различными способами: в электронном виде с использованием выделенных каналов связи (в основном защищенных); в электронном виде с использованием электронной почты; в электронном виде с использованием магнитных носителей информации. Как правило, информационный обмен осуществляется на федеральном уровне через Центральное информационно-техническое таможенное управление (ЦИТТУ).

В целях совершенствования организации информационной безопасности в таможенных органах и организациях, находящихся в ведении ФТС России, действует приказ ФТС России от 28.05.2007 № 660 “О системе антивирусной защиты информации в таможенных органах Российской Федерации”. [/9/](#об_системе_авз) Система антивирусной защиты (АВЗ) информации предназначена для предотвращения заражения программными вирусами информационно-вычислительных ресурсов автоматизированных систем таможенных органов. Практическое выполнение мероприятий по организации антивирусной защиты информации в структурных подразделениях ФТС России и в таможенных органах осуществляет администратор АВЗ, назначаемый соответствующим приказом с обязательным отражением этих обязанностей в должностной инструкции.

Обеспечение информационной безопасности таможенных органов Российской Федерации заключается в создании условий, при которых нанесение вреда элементам системы информационных отношений (свойствам, законным интересам, инфраструктуре или порядку функционирования субъектов информационных отношений) в сфере деятельности таможенных органов становится невозможным или крайне затруднительным.

Защита информации от угроз может быть обеспечена лишь при комплексном подходе к обеспечению информационной безопасности, представляющем собой организационно-правовую совокупность специальных структур, задач, средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа.

Но в данной сфере присутствует ряд проблемных вопросов, а именно низкая степень унификации форматов, способов и регламентов обмена информацией с Федеральными органами исполнительной власти(далее ФОИВ), что связано с недостаточным уровнем развития информационных систем отдельных ФОИВ, а также неготовность ФОИВ представлять Федеральной таможенной службе России необходимую информацию с требуемой степенью актуальности. И в определённой степени сказываются длительные сроки согласования с ФОИВ технических условий информационного взаимодействия для реализации соглашений об информационном обмене между ними.

Таким образом, необходимо совершенствовать механизм межведомственного взаимодействия в целях повышения эффективности реализации функций, стоящих перед таможенными органами.

Лавинообразный рост самых различных киберугроз делает сегодня задачу обеспечения информационной безопасности в государственных структурах актуальной, как никогда.

Что же касается законодательства затрагивающего данную тему, то здесь есть явная необходимость внесения изменений в следующий нормативно правовой акт: п. 4 ч. 3 ст. 5 149-ФЗ “Об информации, информационных технологиях и о защите информации”[/4/,](#тема_2) а именно в данном законе регулирующем отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, не содержится понятия "вредная информация", а используется термин "информация, распространение которой ограничивается или запрещается" (п. 4 ч. 3 ст. 5), однако не указываются цели и причины установленных запретов.

В Законе об информации отсутствует общий перечень видов вредной информации. Так, вся информация, на распространение которой установлен запрет, делится на две большие группы:

1) информация, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды;

2) иная информация, за распространение которой предусмотрена уголовная или административная ответственность (ч. 6 ст. 10).

Указанная норма, на взгляд авторов, не отвечает требованию правовой определенности, поскольку формулировка "иная информация, за распространение которой предусмотрена уголовная или административная ответственность" имеет безразмерный характер, и каждое введение новых запретительных норм в информационной сфере [УК РФ](#уг_код) или [КоАП РФ](#коап) будет увеличивать объем понятия "вредная информация".

БИБЛИОГРАФИЯ

1. Конституция Российской Федерации (принята всенародным   
голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

2. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 17.06.2019) (с изм. и доп., вступ. в силу с 01.07.2019)

3. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 17.06.2019) (с изм. и доп., вступ. в силу с 01.07.2019)

4. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (ред. от 18.03.2019)

5. Федеральный закон от 27.07.2010 N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг" (последняя редакция)

6. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

7. Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (ред. от 22.05.2015)

8. Распоряжение Правительства РФ от 28.12.2012 N 2575-р "О Стратегии развития таможенной службы Российской Федерации до 2020 года" (ред. от 10.02.2018)

9. Приказ ФТС РФ от 28.05.2007 N 660 "О системе антивирусной защиты информации в таможенных органах российской федерации"

10. Обеспечение информационной безопасности таможенных органов РФ Барбышева Г. И., Мирзаев Ш. Ф. // Инновационная экономика: материалы II Международной научной конференции, 2015

11. Недосекова Е.С., Гольтяпина И.Ю., Саввин А.С. Монография: Административно-правовой механизм обеспечения информационной безопасности таможенных органов Российской Федерации. 2013 12. «Облачные» услуги и особенности их правового регулирования в Российской Федерации Елин В.М. // Информационное право, 2017, N 4

13. К вопросу о классификации вредной информации в российском законодательстве Куликова С.А. // Информационное право, 2015, N 4

14. Доктрина информационной безопасности Российской Федерации (новелла законодательства) Молчанов Н.А., Матевосова Е.К. // Актуальные проблемы российского права, 2017, N 2

15. Информационная безопасность и применение технологии блокчейн: зарубежный опыт и необходимость правового регулирования в Российской Федерации Багоян Е.Г. // Юрист, 2019, N 3

16. Информационное пространство: обеспечение информационной безопасности и право. Сб.науч.трудов/Под ред. Т.А Поляковой, В.Б. Наумовой, А.В. Минбалеева. М; ИГП РАН, 2018. – 512 с.

BIBLIOGRAPHY

1. The Constitution of the Russian Federation (adopted by the national

by vote of 12.12.1993) (as amended by the Laws of the Russian Federation on amendments to the Constitution of the Russian Federation of December 30, 2008 No. 6-FKZ, of December 30, 2008 No. 7-FKZ, of February 5, 2014 No. 2-FKZ, of July 21, 2014 No. 11-FKZ).

2. "Criminal Code of the Russian Federation" dated 13.06.1996 N 63-FZ (as amended on June 17, 2019) (as amended and added, entered into force on 07/01/2019)

3. "Code of the Russian Federation on Administrative Offenses" of 19/30/2001 N 195-FZ (as amended on 06/17/2019) (as amended and added, took effect from 07/01/2019)

4. Federal Law of 27.07.2006 N 149-FZ "On Information, Information Technologies and Information Protection" (ed. 03/18/2019)

5. Federal Law of 27.07.2010 N 210-FZ “On the organization of the provision of state and municipal services” (last edited)

6. Presidential Decree of 05.12.2016 N 646 "On approval of the Information Security Doctrine of the Russian Federation"

7. Presidential Decree of 17.03.2008 N 351 “On measures to ensure the information security of the Russian Federation when using information and telecommunication networks of international information exchange” (as amended on 05.22.2015)

8. Order of the Government of the Russian Federation of 28.12.2012 N 2575-p "On the Strategy for the Development of the Customs Service of the Russian Federation up to 2020" (as amended on 10.02.2018)

9. Order of the FCS of the Russian Federation of 28.05.2007 N 660 "On the system of antivirus information protection in the customs bodies of the Russian Federation"

10. Ensuring the information security of the customs authorities of the Russian Federation Barbysheva G. I., Mirzaev Sh. F. // Innovative Economics: Proceedings of the II International Scientific Conference, 2015

11. Nedosekova E.S., Goltyapina I.Yu., Savvin A.S. Monograph: Administrative and legal mechanism for ensuring the information security of the customs authorities of the Russian Federation. 2013

          12. Cloud services and peculiarities of their legal regulation in the Russian Federation Elin V.M. // Information law, 2017, N 4

13. On the issue of classification of harmful information in Russian legislation S. Kulikova. // Information law, 2015, N 4

14. The Doctrine of Information Security of the Russian Federation (the novella of the legislation) Molchanov N.А., Matevosova Ye.K. // Actual problems of Russian law, 2017, N 2

15. Information security and application of the blockchain technology: foreign experience and the need for legal regulation in the Russian Federation Ye. G. Bagoyan // Lawyer, 2019, N 3

16. Information space: information security and law. Sb.nauch.trudov / Ed. T.A Polyakova, V.B. Naumova, A.V. Minbaleeva. M; IHP RAS, 2018. - 512 p.